Docket No: T2147-907679-US 3943

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of	:	
MAURIN J. et al.	:	
Serial No. To be assigned	:	Examiner:
Filed: January 24, 2002	:	Group Art Unit:
For: METHOD AND SYSTEM FOR COMMUNICATING A CERTIFICATE BETWEEN A SECURITY MODULE AND A SERVER	:	McLean, Virginia January 24, 2002

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The following amendments and remarks are submitted prior to examination of the above-identified application on the merits.

IN THE SPECIFICATION

Before the paragraph numbered [0001], insert the following heading:

-- BACKGROUND OF THE INVENTION

1. Field of the Invention.--;

Before the paragraph numbered **[0002]**, delete the header "Prior Art" and insert the following header:

-- 2. Description of the Related Art.--;

Before the paragraph numbered **[0012]**, delete the header "Presentation of the Figures" and insert the following header:

-- BRIEF DESCRIPTION OF THE DRAWINGS --;

Before the paragraph numbered **[0013]**, delete the header "Description of an Embodiment of the Invention" and insert the following header:

-- DESCRIPTION OF THE PREFERRED EMBODIMENTS --;

Page 9, after paragraph **[0055]**, insert the following new paragraph:

--**[0056]** While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims. --;

Page 10, after the header "CLAIMS" and before the first claim, insert the following:

-- We claim: --

IN THE CLAIMS

Please substitute amended claims 1-8 as presented below for the same-numbered claims that were pending prior to the filing of this paper. A marked-up version of the amended claims is attached.

1. (Amended) A method for communicating to a server machine a certificate of a user sent by a client machine via a security module of a computer system, wherein a first protocol used between the client machine and the server machine is an HTTP or an equivalent protocol, and a second security protocol such as SSL or an equivalent protocol is implemented between the client machine and the security module, said method comprising:

inserting said certificate into a cookie header of a request in the first protocol, and

transmitting the request, including said cookie header containing said certificate, from the security module to the server machine.

2. (Amended) A method according to claim 1, further comprising:

removing from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header.

3. (Amended) A method according to claim 1, further comprising:

determining, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine, and

creating a new cookie header if said existing cookie header is not present in the request sent by the client machine.

4. (Amended) A method according to claim 3, further comprising:

adding a specific cookie into the existing or new cookie header, and assigning configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

5. (Amended) A method according to claim 1, further comprising:

transmitting to the server machine the request sent by the client machine into which the certificate has been inserted.

6. (Amended) A security machine for securing exchanges between a client machine and a server machine of a computer system, wherein a first protocol used between the client machine and server machine is an HTTP or an equivalent protocol, and a second security protocol such as SSL or an equivalent protocol is implemented between the client machine and said security machine, said security machine comprising:

an analyzer for enabling the transmission of a certificate into a cookie header of an HTTP or equivalent request.

7. (Amended) A system comprising:

a client machine,

a server machine, and

a security module,

wherein a first protocol used between the client machine and the server

machine is an HTTP or an equivalent protocol, wherein a second security protocol such as SSL or an equivalent protocol is implemented between the client machine and the security module, and wherein the security module comprises an analyzing program for enabling transmission of a certificate sent by the client machine into a cookie header of an HTTP or equivalent request.

8. (Amended) A program integrated into a security module that allows the method according to claim 1 to be executed when the program is run in a machine.

IN THE ABSTRACT

Please replace the Abstract as originally filed with the following new abstract:

-- ABSTRACT --

A network communications method communicates a certificate from a client machine to a server machine through a security module. The protocol used between the client and server machines is HTTP or an equivalent protocol, and a security protocol such as SSL or an equivalent is implemented between the client machine and the security module. The steps of the method include inserting the certificate into a cookie header of a request in HTTP or an equivalent protocol, and then transmitting the request from the security module to the server machine.--

REMARKS

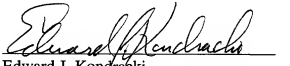
Claims 1-8 are pending. These claims have been amended to place them in a form which comports with U.S. claim practice. Also, the specification has been amended to include section headers and a new abstract has been provided.

It is respectfully submitted that the application is in condition for allowance. Favorable consideration and prompt allowance of the application is respectfully requested.

Should the Examiner believe that further amendments are necessary to place the application in condition for allowance, or if the Examiner believes that a personal interview would be advantageous in order to more expeditiously resolve any remaining issues, the Examiner is invited to contact Applicants' undersigned attorney at the telephone number listed below.

To the extent necessary, Applicants petition for an extension of time under 37 CFR § 1.136. Please charge any shortage in fees due in connection with this application, including extension of time fees, to Deposit Account No. 50-1165 (Attorney Docket No. T2147-907679) and credit any excess fees to the same Deposit Account.

Respectfully submitted,



Edward J. Kondracki
Registration No. 20,604

Miles & Stockbridge P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone No: (703) 610-8641
Facsimile No: (703) 610-8686

Marked-Up Version of the Amended Claims

1. (Amended) A method [Method] for communicating to a server machine [2(b)] a certificate of a user [(4)] sent by a client machine [(2a)] via a security module [(2c)] of a computer system[(1)], [the] wherein a first protocol used between the client machine [(2a)] and the server machine is an [(2b) being] HTTP or an equivalent protocol, and second a security protocol such as [like] SSL or an equivalent protocol [being] is implemented between the client machine [(2a)] and the security module [(2c)], [characterized in that it consists of] said method comprising:

inserting said certificate into a cookie header of a request in [HTTP or an equivalent] the first protocol [in order to transmit], and

transmitting the request, including said cookie header containing said certificate, [them] from the security module [(2c)] to the server machine [(2b)].

2. (Amended) A method [Method] according to claim 1, [characterized in that it consists of] further comprising:

removing from said certificate all [of the] separators used in [the] headers of the [HTTP messages] request prior to [its] insertion of said certificate into said [a] cookie header.

3. (Amended) A method [Method] according to claim 1 [claims 1 and 2], [characterized in that it consists of searching] further comprising:

determining, prior to the [insertion of said certificate into a header] inserting step, [to see if a] whether an existing cookie header is present in the [HTTP] request sent by the client machine [(2a)], and [if not, of]

creating [one] a new cookie header if said existing cookie header is not present in the request sent by the client machine.

4. (Amended) A method [Method] according to claim 3, [characterized in that it consists of] further comprising:

adding a specific cookie into the existing or new [created] cookie header, [a] and assigning configurable default name is assigned to said specific cookie to enable [enabling] the server machine [(2b)] to distinguish the certificate from [the] cookies of the [HTTP or equivalent] request.

5. (Amended) A method [Method] according to [any of claims 1 through 4] claim 1, [characterized in that it consists of] further comprising:

transmitting to the server machine [(2b)] the [HTTP or equivalent] request sent by the client machine [(2a)] into which the certificate has been inserted.

6. (Amended) A security [Security] machine [(2c)] for securing [the] exchanges between a client machine [(2a)] and a server machine [(2b)] of a computer system [(1)], wherein a first [the] protocol used between the client machine [(2a)] and server machine is an [(2b) being] HTTP or an equivalent protocol, and a second security protocol such as [like] SSL or an equivalent protocol is [being] implemented between the client machine [(2a)] and said security machine [(2c)], [characterized in that it comprises] said security machine comprising:

[analyzing means] an analyzer [(6) that make it possible to transmit] for enabling the transmission of a certificate into a cookie header of an HTTP or equivalent request.

7. (Amended) A system [System] comprising:

a client machine [(2a)],

a server machine [(2b)], and

a security module [(2c)],

wherein [the] first protocol used between the client machine [(2a)] and the server machine is an [(2b) being] HTTP or an equivalent protocol, wherein a second security protocol such as [like] SSL or an equivalent protocol [being] is implemented between the client machine [(2a)] and the security module [(2c)], [characterized in that] and wherein the security module [(2c)] comprises an analyzing [means] program [(6) that make it possible to transmit a] for enabling transmission of a certificate sent by the client machine [(2a)] into a cookie header of an HTTP or equivalent request.

8. (Amended) A program [Program] integrated into a security module [(2c)] that allows the method according to claim 1 [any of claims 1 through 5] to be executed when the program is run in a machine.